REMARKS

Claims 1-6 are currently pending in this application, and are at issue herein.

Claims 1-6 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,678,379 to Mayers et al. ("Mayers"). Applicant respectfully traverses the claim rejections for at least the following reasons.

Mayers discloses a method for testing the security of a quantum cryptographic system used for quantum key distribution. The Mayers method utilizes the polarization states of photons, with the photons possessing quantum states satisfying certain relationships between three bases (Mayers, col. 7, line 67 – col. 8, line 20).

The Mayers' method involves a sending party producing a set of three photons in a GHZ state from a GHZ source in a predetermined base. The sending party uses prearranged measurement bases to measure the first and second of the three photons. The third photon is transmitted to the receiving party through a quantum channel, and a receiving party uses a prearranged measurement bases to measure the transmitted photon. The parity of the measurement results for the three photons are collated on a bitwise basis between the sending and receiving parties, and a check is made as to whether or not the parity is correct. After a sufficiently large number of tests have been conducted, it is determined that the quantum key distribution apparatus can be relied upon if the error rate is within a tolerable range (Mayers, col. 8, line 46 – col. 9, line 7).

If the apparatus is found to be reliable, key distribution is performed in Mayers by the sending party again producing a set of three photons in a GHZ state from a GHZ source in a predetermined base. The sending party measures the first and

second of these photons using bases selected from two other predetermined bases at random for each bit, and stores the measurement bases and the results. The third photon is transmitted to the receiving party through the quantum channel, and the receiving party measures the transmitted photon using a base selected from two other predetermined bases at random for each bit, and also stores the measurement bases and the result. The three bases used are then collated between the sending and receiving parties for each bit without telling the measurement results. Of these, it is approximated that half of the bits will correspond to cases where the selected bases constitutes one of four predetermined bases, and these bits are kept and the others are discarded (Mayers, col. 9, lines 8-28).

In Mayers, the sending party and receiving party also extract test bits at random and check whether or not they are correct by collating the parity of the bit values for each bit. If this test produces correct parities for a sufficient number of bits, Mayers concludes that there is no eavesdropping activity, and the test bits are discarded and a shared key is produced from the remaining random series of bits (Mayers, col. 9, lines 29-41).

In contrast, the present invention concerns a key arrangement method including a first system which encodes a bit sequence and sends it to a second system. The second system decodes the received signals and measures the signal values. The second system records some second values, which are above a predetermined value, and tells the first system bit positions of the selected bits. The first system selects values corresponding to those bit positions, and discards the rest of them.

In comparing the present invention to Mayers, it is clear that Mayers does not adopt only bits having a measured value beyond a threshold value. As disclosed in Mayers, if a sufficient number of bits meet a parity test, it is concluded that there is no eavesdropping activity. The bits that have been tested are discarded, and a shared key is produced from the remaining random series of bits (Mayers, col. 9, lines 29-36). In contrast, and as recited in claim 1, the second system adopts only those bits having a measured value beyond the threshold value, and informs the first system of the bit positions of the selected bits. The adopted bits are then used as a key string for the first and second systems. Mayers discloses to discard the bits that are actually tested, and utilize the remaining random series of bits to form the shared key.

Further, in the present invention, it is the second system that determines which bits to use for the key string. In contrast, Mayers discloses that the parity of the measurement results are collated on a bitwise basis between the sending and receiving parties. Thus, both the sending and receiving parties in Mayers are involved in the testing procedure.

Accordingly, for at least the above-identified reasons, Applicant submits that claim 1 is allowable over Mayers.

Claims 2-6 depend cognantly from independent claim 1, recite further structural limitations for the delineating over the prior art, and are also believed allowable. A discussion of the dependent claims will not be belabored for the sake of brevity.

Conclusion

Based on the reasons as set forth above, Applicant respectfully requests allowance of all pending claims including claims 1-6.

In the event that there are any questions concerning this paper, or the application in general, the Examiner is respectfully urged to telephone Applicants' undersigned representative so that prosecution of the application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: January 19, 2006

By: _____
Charles F. Wieland III
Registration No. 33,096

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620